PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2003-016037**
(43)Date of publication of application : **17.01.2003**

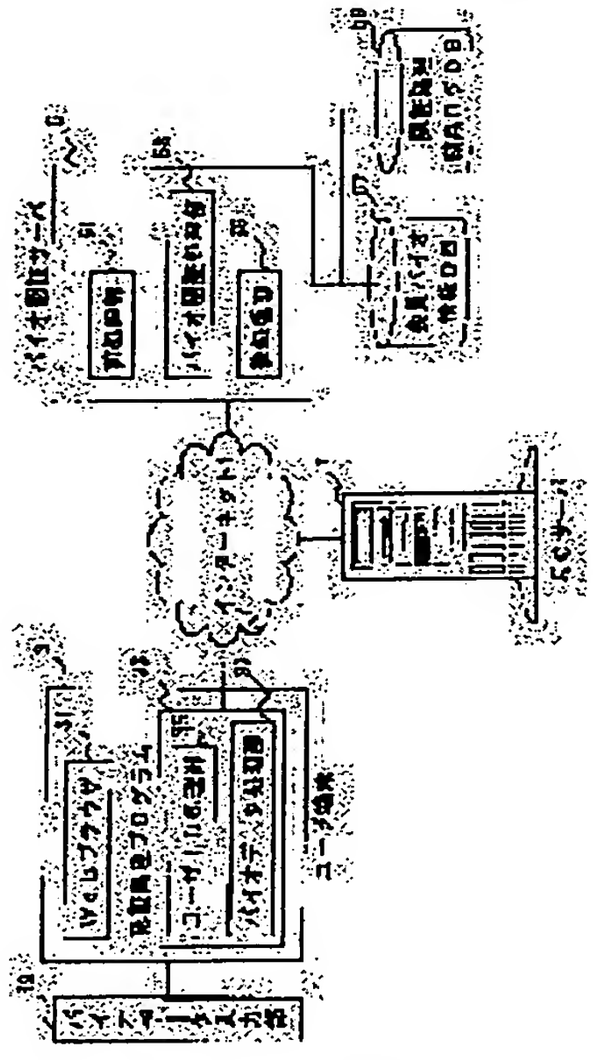
(51)Int.CI. **G06F 15/00**
H04L 9/32

(21)Application number : **2001-198141**
(22)Date of filing : **29.06.2001**

(71)Applicant : **NIFTY CORP**
(72)Inventor : **TAWARA TADAYUKI**

(54) METHOD FOR AUTHENTICATION PROCESSING

(57)Abstract:
PROBLEM TO BE SOLVED: To safely perform biometric authentication processing at a user terminal in a system comprising a center server and a user terminal.
SOLUTION: User information is acquired according to a request from an EC(electronic commerce) server 7 to be transmitted to a bio authentication server 5, an input of biometric data from a user is prompted. When receiving the registered data from the server 5, the processing is performed by using the inputted data by the user and the received registered data to transmit a result of the processing to the server 7. When receiving a request for the biometric data from the server 5, the biometric data inputted from the user is transmitted to the server 5.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁(JP)

(12)公開特許公報（A）

(11)特許出願公開番号

特開２００３－１６０３７

（Ｐ２００３－１６０３７Ａ）

(43)公開日　平成15年1月17日(2003.1.17)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０　Ｂ	5B085
					３３０　Ｆ	5J104
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７３　Ｄ	

審査請求　未請求　請求項の数１０　ＯＬ　（全１２頁）

(21)出願番号　特願2001-198141(P2001-198141)

(22)出願日　平成13年6月29日(2001.6.29)

(71)出願人　591117192
ニフティ株式会社
東京都品川区南大井6－26－1

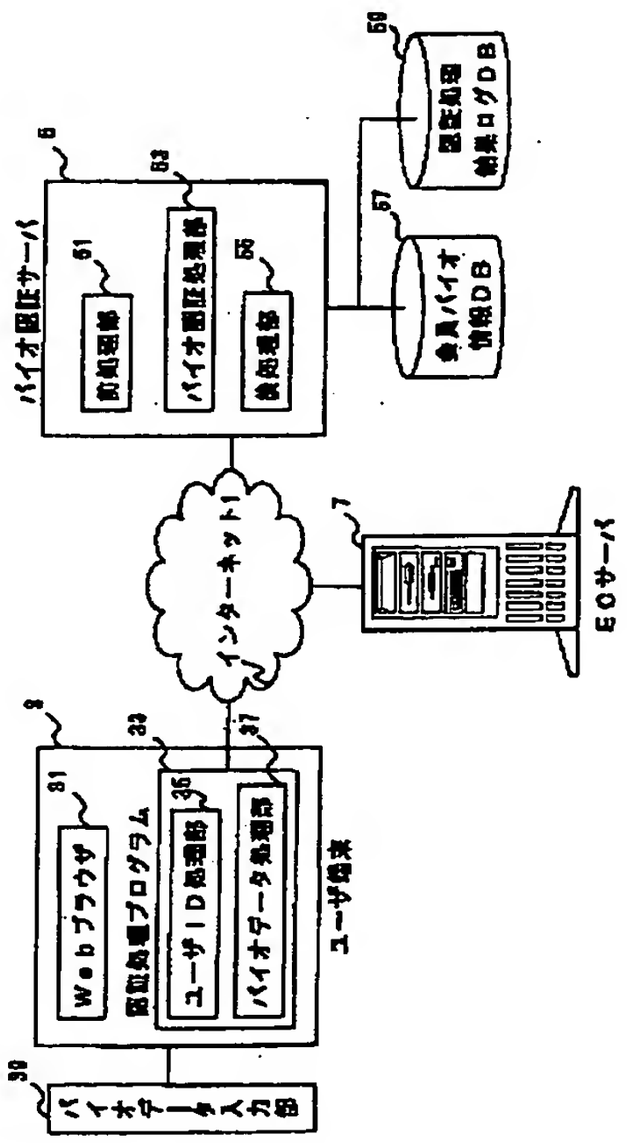
(72)発明者　田原　忠行
東京都品川区南大井六丁目26番1号　ニフティ株式会社内

(74)代理人　100103528
弁理士　原田　一男

Ｆターム(参考)　5B085 AE02 AE04 AE09 AE23 AE25
5J104 AA07 KA01 KA16 KA17 KA18
MA04 PA07 PA10

(54)【発明の名称】認証処理方法

(57)【要約】
【課題】センタ・サーバとユーザ端末とを含むシステムにおいてユーザ端末においてバイオメトリクス認証処理を安全に実施する。
【解決手段】ＥＣサーバ７からの要求に応じて、ユーザ識別情報を取得してバイオ認証サーバ５に送信する。また、ユーザに対してバイオメトリクス・データの入力を促す。倍認証サーバ５から登録バイオメトリクス・データを受信すると、ユーザにより入力されたバイオメトリクス・データとバイオ認証サーバ５から受信した登録バイオメトリクス・データとを用いて、バイオメトリクス認証処理を実施する。そして、バイオメトリクス認証処理の結果を、ＥＣサーバ７に送信する。また、バイオメトリクス認証処理の結果を、バイオ認証サーバ５に送信し、バイオ認証サーバ５からバイオメトリクス・データの要求を受信した場合には、ユーザにより入力されたバイオメトリクス・データをバイオ認証サーバ５に送信する。



【特許請求の範囲】
【請求項１】認証結果要求元コンピュータからの要求に応じて、ユーザ識別情報を取得してセンタ・サーバに送信するユーザ識別情報送信ステップと、
ユーザに対してバイオメトリクス・データの入力を促すステップと、
前記センタ・サーバから登録バイオメトリクス・データを受信するステップと、
前記ユーザにより入力されたバイオメトリクス・データと前記センタ・サーバから受信した登録バイオメトリクス・データとを用いて、バイオメトリクス認証処理を実施するステップと、
前記バイオメトリクス認証処理の結果を、前記認証結果要求元コンピュータに送信するステップと、
を含む認証処理方法。
【請求項２】前記バイオメトリクス認証処理の結果を、前記センタ・サーバに送信するステップと、
前記センタ・サーバからバイオメトリクス・データの要求を受信した場合には、前記バイオメトリクス認証処理において用いられたバイオメトリクス・データを前記センタ・サーバに送信するステップと、
をさらに含む請求項１記載の認証処理方法。
【請求項３】前記センタ・サーバから前記登録バイオメトリクス・データの代わりにバイオメトリクス・データ送信要求を受信した場合には、前記ユーザの入力にかかるバイオメトリクス・データを前記センタ・サーバに送信するステップをさらに含む請求項１又は２記載の認証処理方法。
【請求項４】前記ユーザ識別情報送信ステップが、
ユーザ機器の固有情報、又は前記ユーザにより予め入力された識別情報のいずれかを前記ユーザ識別情報として取得して前記センタ・サーバに送信するステップを含む請求項１乃至３のいずれか１つ記載の認証処理方法。
【請求項５】ユーザ端末からユーザ識別情報を受信するステップと、
前記ユーザ識別情報を用いて、登録バイオメトリクス・データを登録バイオメトリクス情報ＤＢから取り出し、前記ユーザ端末に送信するステップと、
前記ユーザ端末から前記登録バイオメトリクス情報に基づく認証結果を受信し且つ当該認証結果が認証成功を示している場合、前記登録バイオメトリクス・データの更新をすべきか判断するステップと、
更新すべきと判断された場合には、前記ユーザ端末にバイオメトリクス・データ要求を送信するステップと、
を含む認証処理方法。
【請求項６】ユーザ端末からユーザ識別情報を受信するステップと、
ユーザ端末におけるバイオメトリクス認証処理又はセンタ・サーバにおけるバイオメトリクス認証処理のいずれを実施するか決定するステップと、

前記ユーザ端末におけるバイオメトリクス認証処理を実施すると決定された場合には、前記ユーザ識別情報に対応する登録バイオメトリクス・データを取得して前記ユーザ端末に送信するステップと、
前記センタ・サーバにおけるバイオメトリクス認証処理を実施すると決定された場合には、バイオメトリクス・データ要求を前記ユーザ端末に送信するステップと、
を含む認証処理方法。
【請求項７】請求項１乃至６のいずれか１つに記載された認証処理方法をコンピュータに実行させるためのコンピュータ・プログラム。
【請求項８】認証結果要求元コンピュータからの要求に応じて、ユーザ識別情報を取得してセンタ・サーバに送信する手段と、
ユーザに対してバイオメトリクス・データの入力を促す手段と、
前記センタ・サーバから登録バイオメトリクス・データを受信する手段と、
前記ユーザにより入力されたバイオメトリクス・データと前記センタ・サーバから受信した登録バイオメトリクス・データとを用いて、バイオメトリクス認証処理を実施する手段と、
前記バイオメトリクス認証処理の結果を、前記認証結果要求元コンピュータに送信する手段と、
を有するコンピュータ。
【請求項９】ユーザ端末からユーザ識別情報を受信する手段と、
前記ユーザ識別情報を用いて、登録バイオメトリクス・データを登録バイオメトリクス情報ＤＢから取り出し、前記ユーザ端末に送信する手段と、
前記ユーザ端末から前記登録バイオメトリクス・データに基づく認証結果を受信し且つ当該認証結果が認証成功を示している場合、前記登録バイオメトリクス・データの更新をすべきか判断する手段と、
更新すべきと判断された場合には、前記ユーザ端末にバイオメトリクス・データ要求を送信する手段と、
を有するコンピュータ・システム。
【請求項１０】ユーザ端末からユーザ識別情報を受信する手段と、
ユーザ端末におけるバイオメトリクス認証処理又はセンタ・サーバにおけるバイオメトリクス認証処理のいずれを実施するか決定する手段と、
前記ユーザ端末におけるバイオメトリクス認証処理を実施すると決定された場合には、前記ユーザ識別情報に対応する登録バイオメトリクス・データを取得して前記ユーザ端末に送信する手段と、
前記センタ・サーバにおけるバイオメトリクス認証処理を実施すると決定された場合には、バイオメトリクス・データ要求を前記ユーザ端末に送信する手段と、
を有するコンピュータ・システム。

【発明の詳細な説明】

【０００１】

【発明が属する技術分野】本発明は、バイオメトリクス認証処理技術に関する。

【０００２】

【従来の技術】従来、ネットワークを介したバイオメトリクス認証処理は、ユーザ端末から認証サーバにバイオメトリクス・データ（以下、バイオ・データとも呼ぶ）を送信し、当該認証サーバにおいてバイオ・データを用いた認証処理を実施していた。また、認証サーバに登録されたバイオ・データは、ユーザが希望したときにのみ登録変更が行われる構成であった。

【０００３】

【発明が解決しようとする課題】従来技術によれば、バイオ・データはデータ・サイズが大きく、且つ認証サーバでの解析には比較的大きな処理能力が必要とされる。また、バイオ・データのユーザ端末から認証サーバへの送信は、通信回線品質や音量などにより認証サーバで解析が可能となるレベルになるまで何回も要求される場合もあり、通信回線網や認証サーバの負担が大きかった。従って、多くのユーザが認証サーバに一度にアクセスすると、処理時間が長くなったり、クラッカーによる大量の不正データ送付（いわゆるＤｏＳ攻撃（Denied of Service attack）によるサーバ麻痺の危険性があった。

【０００４】これらの問題は主に認証サーバにおいてバイオメトリクス認証処理を実施するための生ずるものである。

【０００５】従って、本発明の目的は、センタ・サーバとユーザ端末とを含むシステムにおいてユーザ端末においてバイオメトリクス認証処理を実施するための技術を提供することである。

【０００６】他の目的は、センタ・サーバにおいて必要な時に登録されたバイオメトリクス・データの更新を要求を行うことができるようにするための技術を提供することである。

【０００７】さらに他の目的は、センタ・サーバとユーザ端末とを含むシステムにおいてユーザ端末においてバイオメトリクス認証処理を安全に実施するための技術を提供することである。

【０００８】

【課題を解決するための手段】本発明の第１の態様に係る、ユーザ端末（例えば実施の形態におけるユーザ端末３）における認証処理方法は、認証結果要求元コンピュータ（例えば実施の形態におけるＥＣサーバ７）からの要求に応じて、ユーザ識別情報を取得してセンタ・サーバ（例えば実施の形態におけるバイオ認証サーバ５）に送信するユーザ識別情報送信ステップと、ユーザに対してバイオメトリクス・データの入力を促すステップと、センタ・サーバから登録バイオメトリクス・データを受信するステップと、ユーザにより入力されたバイオメトリクス・データとセンタ・サーバから受信した登録バイオメトリクス・データとを用いて、バイオメトリクス認証処理を実施するステップと、バイオメトリクス認証処理の結果を、認証結果要求元コンピュータに送信するステップとを含む。

【０００９】このようにすれば、センタ・サーバの処理負荷は大幅に減少でき、クラッカー等によるＤｏＳ攻撃に対処しやすくなる。また、バイオメトリクス・データについては、一度だけネットワークを介して送信されるだけであるから、ネットワークの負荷も下げることができる。さらに、ＡＤＳＬ（Asymmetric Digital Subscriber Line）をユーザが用いている場合には、サイズの大きいバイオメトリクス・データのダウンロードも高速に行うことができる。なお、バイオメトリクス認証には、ユーザの顔による顔認証、音声認証、指紋認証、サイン認証などが含まれる。

【００１０】また、本発明の第１の態様において、バイオメトリクス認証処理の結果を、センタ・サーバに送信するステップと、センタ・サーバからバイオメトリクス・データの要求を受信した場合には、バイオメトリクス認証処理において用いられたバイオメトリクス・データをセンタ・サーバに送信するステップとをさらに含むような構成であってもよい。

【００１１】これにより、センタ・サーバにおいては、ユーザのバイオメトリクス・データの経年変化に対応して登録バイオメトリクス・データの更新を行うことができるようになる。

【００１２】さらに、本発明の第１の態様において、センタ・サーバから登録バイオメトリクス・データの代わりにバイオメトリクス・データ送信要求を受信した場合には、ユーザの入力にかかるバイオメトリクス・データをセンタ・サーバに送信するステップをさらに含むような構成であってもよい。常にユーザ端末においてバイオメトリクス認証処理を実施するとすると、悪意を持ったユーザが不正な行為を行うこともあるので、例えばランダムに、又はセンタ・サーバの処理負荷状態等に応じて、センタ・サーバにおけるバイオメトリクス認証を実施するようにすれば、不正を防止することができるようになる。

【００１３】さらに、上で述べたユーザ識別情報送信ステップが、ユーザ機器の固有情報（例えばＭＡＣアドレス、ＣＰＵのシリアル番号など）、又はユーザにより予め入力された識別情報のいずれかをユーザ識別情報として取得してセンタ・サーバに送信するステップを含むような構成であってもよい。例えば、会員ＩＤ以外の識別情報、特にユーザ機器の固有情報等であれば、不正取得の可能性が低くなり、安全な認証処理が行われることとなる。

【００１４】本発明の第２の態様に係る、センタ・サーバにおける認証処理方法は、ユーザ端末からユーザ識別

情報を受信するステップと、ユーザ識別情報を用いて、登録バイオメトリクス・データを登録バイオメトリクス情報ＤＢから取り出し、ユーザ端末に送信するステップと、ユーザ端末から登録バイオメトリクス・データに基づく認証結果を受信し且つ当該認証結果が認証成功を示している場合、登録バイオメトリクス・データの更新をすべきか判断するステップと、更新すべきと判断された場合には、ユーザ端末にバイオメトリクス・データ要求を送信するステップとを含む。

【００１５】このようにすればセンタ・サーバは、登録バイオメトリクス・データを適切な時期に更新することができるようになる。

【００１６】本発明の第３の態様に係る、センタ・サーバにおける認証処理方法は、ユーザ端末からユーザ識別情報を受信するステップと、ユーザ端末におけるバイオメトリクス認証処理又はセンタ・サーバにおけるバイオメトリクス認証処理のいずれを実施するか決定するステップと、ユーザ端末におけるバイオメトリクス認証処理を実施すると決定された場合には、ユーザ識別情報に対応する登録バイオメトリクス・データを取得してユーザ端末に送信するステップと、センタ・サーバにおけるバイオメトリクス認証処理を実施すると決定された場合には、バイオメトリクス・データ要求をユーザ端末に送信するステップとを含む。このような構成によりユーザの不正行為の抑止効果を期待することができるようになる。

【００１７】また、本発明の第１乃至３の態様に係る方法をコンピュータに実行させるためのプログラムを作成することも可能であって、当該プログラムは、例えばフレキシブル・ディスク、ＣＤ－ＲＯＭ、光磁気ディスク、半導体メモリ、ハードディスク等の記憶媒体又は記憶装置に格納される。なお、ネットワークを介して配布される場合もある。また、処理途中のデータについては、コンピュータのメモリに一時保管される。

【００１８】

【発明の実施の形態】本発明の一実施の形態に係るシステム概要を図１に示す。コンピュータ・ネットワークであるインターネット１には、１又は複数のユーザ端末３と、バイオ認証サーバ５と、１又は複数のＥＣ（Electronic Commerce）サーバ７とが接続されている。

【００１９】ユーザ端末３には、例えばウェブ（Ｗｅｂ）ブラウザ３１がインストールされており、Ｗｅｂサーバ機能を有するＥＣサーバ７との間でＨＴＴＰ（Hyper TextTransfer Protocol）に従って通信を行い、受信したＷｅｂページ・データ（例えばＨＴＭＬ（Hyper Text Markup Language）ファイルや参照されている場合には画像ファイルを含む）を表示装置に表示する。また、ユーザ端末３には、本実施の形態において主な処理を実施する認証処理プログラム３３もインストールされている。この認証処理プログラム３３は、例えばＷｅｂブラウザ３１のプラグイン（Plug-in）プログラムとして会員（登録ユーザ）に配布されるような場合もあれば、Ｗｅｂブラウザ３１と連携する別のプログラムとして会員（登録ユーザ）に配布されるような場合もある。

【００２０】認証処理プログラム３３には、会員ＩＤやその他のユーザ識別情報を処理するユーザＩＤ処理部３５と、ユーザにバイオ・データの入力を行わせるための処理、当該バイオ・データとバイオ認証サーバ５から受信した登録バイオ・データを用いた認証処理、バイオ認証サーバ５からの要求に応じて入力バイオ・データをバイオ認証サーバ５に送信する処理等を実施するバイオデータ処理部３７とが含まれる。

【００２１】ユーザ端末３には、バイオデータ入力部３９が接続されている。例えば顔認証の場合、このバイオデータ入力部３９は顔の画像データを取得するためのカメラである。また、音声認証の場合には、音声を電気信号に変換するマイクロフォンである。指紋認証の場合には、指紋読取装置である。サイン認証の場合には、手書き文字の入力を行うためのデジタイザ等の座標入力装置である。その他のバイオメトリクス認証処理の場合には、それに対応する入力装置である。これらの装置については従来と同じであるから、これ以上説明しない。

【００２２】ＥＣサーバ７は、Ｗｅｂサーバ機能を有する電子商取引を行うためのサーバである。多くの店舗が出店されている電子モールであってもよいし、一つの店舗のためのだけのＥＣサーバであってもよい。ＥＣサーバ７の構成は、バイオ認証処理に関係する、ユーザ端末３及びバイオ認証サーバ５とのインターフェースの部分のみが従来と異なる部分である。これについては、以下で説明する処理フローにて明らかにする。

【００２３】バイオ認証サーバ５には、前処理部５１と、バイオメトリクス認証処理を実施するバイオ認証処理部５３と、後処理部５５とが含まれる。各処理部の処理内容については後に説明する。また、バイオ認証サーバ５は、会員ＩＤを含む会員の個人情報と、バイオ・データとを格納する会員バイオ情報データベース（ＤＢ）５７と、認証処理結果ログＤＢ５９とを管理している。なお、ユーザは、予め何らかの方法にてバイオ認証サーバ５に会員の個人情報とバイオ・データとの登録を行っておく必要がある。例えば、会員登録用のＷｅｂサーバ及びユーザ端末３を用いて又は申込書を用いて会員登録の申し込みを行い、バイオ・データを電話や店舗における直接の登録や郵送による登録を行う。

【００２４】次に図２乃至図５を用いて図１に示されたシステムの処理フローを説明する。ユーザは、ＥＣサーバ７の例えばショッピングカートのＷｅｂページに設けられた購入ボタン等をクリックする。また、ログインが必要なページへのリンクをクリックするような場合もある。そうすると、ユーザ端末３は、ＥＣサーバ７の認証処理が必要となるＷｅｂページへアクセスする（ステッ

プＳ１）。ＥＣサーバ７は、このアクセスに応答してバイオ認証サーバ５へのＩＤ送信要求を、ユーザ端末３に送信する（ステップＳ３）。この際、後に本実施の形態に従って認証処理が行われたことを確認するための第１キーを生成して、ユーザ端末３及びバイオ認証サーバ５に送信する場合もある。ユーザ端末３及びバイオ認証サーバ５は、第１キーを受信し、記憶装置に格納しておく。

【００２５】ユーザ端末３は、ＩＤ送信要求をＥＣサーバ７から受信すると（ステップＳ５）、認証処理プログラム３３を起動する。認証処理プログラム３３のユーザＩＤ処理部３５は、ＩＤの自動送信が指定済みであるか確認する（ステップＳ７）。もし、ＩＤの自動送信が指定されていない場合にはステップＳ１９に移行する。一方、ＩＤの自動送信が指定されている場合には、送信すべきＩＤが会員ＩＤであるか否かを判断する（ステップＳ９）。もし、会員ＩＤである場合にはステップＳ１７に移行する。会員ＩＤではない場合には、ユーザ端末固有の情報の自動取得が指定されているか否かを判断する（ステップＳ１１）。ユーザ端末固有の情報とは、例えばＭＡＣ（Media Access Control）アドレスやＣＰＵのシリアル番号等である。例えば認証処理プログラム３３をインストール時等に、これらの情報の使用をユーザが許可し、且つ例えばインターネット１等を経由してバイオ認証サーバ５に予め登録しているものとする。すなわち、会員バイオ情報ＤＢ５７には、会員ＩＤと機器固有情報との対応関係が記録されている。

【００２６】もし、ユーザ端末固有情報の自動取得が指定されていれば、認証処理プログラム３３は、ユーザ端末３のユーザ端末固有情報（ＩＤとも呼ぶ）を自動で取得する（ステップＳ１３）。一方、ユーザ端末固有情報の自動取得が指定されていない場合には、認証処理プログラム３３のインストール時に入力された固有情報（ＩＤとも呼ぶ）を取得する（ステップＳ１５）。この固有情報は、例えば認証処理プログラム３３がインストール時にユーザにより指定された情報である。ユーザ端末固有情報そのものであっても良いし、ユーザにより変更等された情報であってもよい。ステップＳ１３及びステップＳ１５の後にステップＳ２１に移行する。

【００２７】ステップＳ９で送信すべきＩＤは会員ＩＤであると判断された場合には、認証処理プログラム３３のインストール時に入力された会員ＩＤを取得する（ステップＳ１７）。そして、ステップＳ２１に移行する。ステップＳ７でＩＤの自動送信が指定されてない場合には、会員ＩＤの入力を促し、ユーザが入力した会員ＩＤを取得する（ステップＳ１９）。

【００２８】このようにステップＳ１３、ステップＳ１５、ステップＳ１７、又はステップＳ１９において取得されたＩＤを、認証処理プログラム３３は、暗号化して、バイオ認証サーバ５に送信する（ステップＳ２１）。バイオ認証サーバ５の前処理部５１は、ユーザ端末３から暗号化されたＩＤを受信する（ステップＳ２３）。このユーザ端末３の認証処理プログラム３３とバイオ認証サーバ５との通信は、専用のプロトコルを用いるようにしても良い。この場合には、悪意のあるユーザによるなりすまし等の攻撃を受けにくくなる。なお、キーを用いてなりすまし等を防止する場合には、認証処理プログラム３３は、ＥＣサーバ７により付与された第１キーをＩＤと共に隠しパラメータとして送信する。この場合、バイオ認証サーバ５は、第１キーを受信すると、ＥＣサーバ７から受信された第１キーと照合する。もし、ユーザ端末３から受信した第１キーと例えば所定時間内にＥＣサーバ７から受信された第１キーとのマッチングが取れない場合には、当該受信したＩＤを無視する、又は無効としてユーザ端末３に通知する。

【００２９】端子Ａ、端子Ｂ及び端子Ｃを介して図３に移行する。

【００３０】前処理部５１は、暗号化されたＩＤを復号化し（ステップＳ２５）、バイオ認証サーバ５で認証処理を実施するか否かを判断する（ステップＳ２７）。もし、バイオ認証サーバ５で認証処理を実施する場合には、端子Ｅを介して図５に移行する。バイオ認証サーバ５で認証処理を実施するか否かは、様々な要素で決定され得る。例えば、ランダムであってもよい。また、バイオ認証サーバ５の処理負荷レベルで決定しても良い。例えば、処理負荷レベルが高い場合にはユーザ端末３において認証処理を実施し、低い場合にはバイオ認証サーバ５で処理するような場合もある。さらに、同一ユーザにつき所定回数ごとにバイオ認証サーバ５で実施するようにしても良い。また、特定のユーザについては常にバイオ認証サーバ５、逆に特定のユーザについては常にユーザ端末３でバイオ認証処理を実施するようにしても良い。さらに、ＥＣサーバ７から指定を受けるような構成であってもよい。例えば、値段が高い場合や特定の商品の場合にはＥＣサーバ７からバイオ認証サーバ５における認証処理を要求するような構成であってもよい。

【００３１】もし、ユーザ端末３における認証処理を実施すると判断された場合には、前処理部５１は、受信したＩＤに対応する登録バイオ・データを会員バイオ情報ＤＢ５７から読み出し（ステップＳ２９）、当該登録バイオ・データを暗号化して、当該暗号化登録バイオ・データをユーザ端末３に送信する（ステップＳ３１）。登録バイオ・データは、ユーザ端末３にインストールされた認証処理プログラム３３のバイオデータ処理部３７において行われる認証処理において使用しやすい形式に変形されたデータ（例えばモデル・データや特徴データ）である場合もある。なお、キーを用いた処理系である場合には、ここで第２キーを生成してユーザ端末３に暗号化登録バイオ・データと共に送信する場合もある。また、第１及び第２のキーをＥＣサーバ７に送信しておく

場合もある。これによりＥＣサーバ７は、注文情報やＥＣサイトにおけるユーザの識別情報等と第１及び第２キーの対応付けができるようになる。ユーザ端末３及びＥＣサーバ７は、キーを受信し、記憶装置に格納する。

【００３２】一方、ユーザ端末３では、バイオデータ処理部３７が、ユーザに対してバイオ・データの入力を要求する（ステップＳ３３）。これに対してユーザは、バイオデータ入力部３９に対してバイオ・データを入力し、バイオデータ処理部３７が当該バイオ・データを取得する（ステップＳ３５）。そして、バイオデータ処理部３７は、バイオ認証サーバ５から暗号化登録バイオ・データを受信する（ステップＳ３７）。また、バイオデータ処理部３７は、暗号化登録バイオ・データを復号化し、登録バイオ・データを復元する（ステップＳ３９）。そして、登録バイオ・データと入力バイオ・データとを用いて認証処理を実施する（ステップＳ４１）。この認証処理については、バイオ・データの種類により異なり且つ基本的に従来と同じであるからここでは説明を省略する。

【００３３】そしてバイオデータ処理部３７は、認証が成功したか判断する（ステップＳ４３）。もし認証に失敗したと判断された場合には、端子Ｆを介して図４に移行する。一方、認証に成功したと判断された場合には、認証成功をＥＣサーバ７及びバイオ認証サーバ５に送信する（ステップＳ４５）。もしキーを用いた処理系の場合には、第２キーを隠しパラメータとしてＥＣサーバ７及びバイオ認証サーバ５に送信する。ＥＣサーバ７は、第２キーをユーザ端末３から受信するとバイオ認証サーバ５から受信した第２キーと照合して、正規の処理フロー（特にステップＳ３１）を経て認証成功が通知されているかを確認する。もし、ＥＣサーバ７はバイオ認証サーバ５から同一の第２キーを受信していない場合には認証成功としては取り扱わない場合もある。バイオ認証サーバ５についても同様である。

【００３４】ＥＣサーバ７は、ユーザ端末３から認証成功の情報を受信し（ステップＳ４７）、認証後の処理を実施する（ステップＳ４９）。認証後の処理とは、例えば申込受け付け通知を送信したり、決済ページを送信したり、実際に決済処理を実行したりする処理である。但し、これに限定されるものではない。

【００３５】バイオ認証サーバ５の前処理部５１は、ユーザ端末３から認証成功の情報を受信し（ステップＳ５１）、認証日時を認証処理結果ログＤＢ５９に登録する（ステップＳ５３）。例えば、認証成功の情報にＥＣサーバ７についての情報が含まれる場合には、当該情報も認証処理結果ログＤＢ５９に格納しても良い。次に、後処理部５５は、登録バイオ・データの更新時期になったか否かを判断する（ステップＳ５５）。例えば、所定周期ごとに登録バイオ・データを更新することになっている場合には、当該所定周期を経過したか否かを更新記録などを参照して判断する。

【００３６】もし、登録バイオ・データの更新時期ではないと判断された場合には、処理を終了する。一方、登録バイオ・データの更新時期であると判断された場合には、後処理部５５はユーザ端末３にバイオデータ要求を送信する（ステップＳ５７）。ユーザ端末３のバイオデータ処理部３７は、バイオデータ要求を受信し（ステップＳ５９）、ステップＳ３５で取得したバイオ・データ又はステップＳ４１における認証処理において処理されたバイオ・データのいずれかを暗号化し、バイオ認証サーバ５に送信する（ステップＳ６１）。バイオ認証サーバ５の後処理部５５は、ユーザ端末３から暗号化バイオ・データを受信し、復号化して、会員バイオ情報ＤＢ５７に登録する（ステップＳ６３）。なお、受信したバイオ・データにさらに処理を施した後に登録することもある。例えば、モデル・データや特徴データを抽出する処理である。さらに、なりすまし等を防止するために、バイオ認証処理部５３で認証処理を実施し、認証成功を確認した上で登録するようにしてもよい。

【００３７】次に、ステップＳ４３において認証失敗と判断された場合（端子Ｆ経由）の処理を図４を用いて説明する。認証失敗の場合には、バイオデータ処理部３７は認証処理回数は許容限度内（例えば３回）であるか判断する（ステップＳ６５）。もし、認証処理回数が許容限度内であれば、端子Ｄを介して図３のステップＳ３３に戻り、ユーザによるバイオ・データの入力を再度求め、再度入力されたバイオ・データを用いて認証処理を実施する。一方、認証処理回数が許容限度を超えていれば、認証失敗をＥＣサーバ７及びバイオ認証サーバ５に送信する（ステップＳ６７）。もし、キーを用いた処理系の場合には、このときに隠しパラメータとして第２キーを合わせて送信する。

【００３８】ＥＣサーバ７は、ユーザ端末３から認証失敗を受信すると（ステップＳ６９）、認証要求を無効として取り扱う（ステップＳ７１）。すなわち、発注受付を送信しないようにしたり、決済を実行したりせず、今回は受け付けられない旨の通知を行ったりする。また、バイオ認証サーバ５の前処理部５１は、認証失敗の情報を受信し（ステップＳ７３）、当該認証失敗を認証処理結果ログＤＢ５９に登録する（ステップＳ７５）。これで処理を終了する。

【００３９】これによりユーザ端末３における認証処理が安全に行われる。またネットワークの負荷を軽減でき、且つバイオ認証サーバ５の処理負荷を減らすことができるようになる。さらに、バイオ認証サーバ５における処理負荷を減らすことができるので、ＤｏＳ攻撃などの対処がしやすくなる。また、ユーザ端末３にインストールされる専用の認証処理プログラム３３を用いるためにハッキング等を受けることが少なくなる。さらに、バイオ認証サーバ５の会員バイオ情報ＤＢ５７に登録され

るバイオ・データを時々更新することにより、バイオ・データの経年変化に対応できるようになる。

【００４０】次に図５を用いて図３のステップＳ２７でバイオ認証サーバ５で認証処理を実施すると判断された場合（端子Ｅ経由）の処理を説明する。前処理部５１がバイオ認証サーバ５で認証処理を実施すると判断すると、バイオ・データの送信要求をユーザ端末３に送信する（ステップＳ８１）。もし、キーを用いる処理系の場合には、第２キーを生成して、ユーザ端末３に第２キーを隠しパラメータとして送信する。ユーザ端末３は第２キーを受信し、記憶装置に格納する。また、第１及び第２キーをＥＣサーバ７に送信する。ＥＣサーバ７は第１及び第２キーを受信し、記憶装置に格納する。

【００４１】ユーザ端末３のバイオデータ処理部は、バイオ認証サーバ５からバイオ・データの送信要求を受信し（ステップＳ８３）、ユーザによりバイオデータ入力部３９から入力されたバイオ・データ又はバイオ認証サーバ５における認証処理に適した形式に変形したバイオ・データを暗号化し、バイオ認証サーバ５に送信する（ステップＳ８５）。もし、キーを用いる処理系の場合には、第２キーを隠しパラメータとしてバイオ認証サーバ５に送信する。第２キーを受信したバイオ認証サーバ５のバイオ認証処理部５３は、第２キーの照合を行って、適正なユーザ端末３から暗号化入力バイオ・データを受信したことを確認する。

【００４２】バイオ認証サーバ５のバイオ認証処理部５３は、ステップＳ８１の後にＩＤに対応する登録バイオ・データを会員バイオ情報ＤＢ５７から読み出す（ステップＳ８７）。また、ユーザ端末３から暗号化入力バイオ・データを受信し、復号化処理を実施する（ステップＳ８９）。そして、バイオ認証処理部５３は、登録バイオ・データと入力バイオ・データを用いて認証処理を実施する（ステップＳ９１）。この認証処理については、バイオ・データの種類により異なり且つ基本的に従来と同じであるからここでは説明を省略する。

【００４３】そして、バイオ認証処理部５３は認証処理の結果が成功を示しているか判断する（ステップＳ９３）。もし、失敗を示している場合にはステップＳ１０９に移行する。一方、認証処理の結果が成功を示している場合には、認証成功をユーザ端末３及びＥＣサーバ７に送信する（ステップＳ９５）。ＥＣサーバ７は、バイオ認証サーバ５から認証成功の情報を受信すると（ステップＳ９７）、認証後の処理、例えば発注受付通知の処理や、決済ページの情報をユーザ端末３へ送信する処理、又は決済処理自体を実施する（ステップＳ９９）。また、ユーザ端末３は、バイオ認証サーバ５から認証成功の情報を受信する（ステップＳ１０１）。もし、キーを用いた処理系の場合には、バイオ認証サーバ５のバイオ認証処理部５３はＥＣサーバ７に隠しパラメータとして第２キーを送信する。ＥＣサーバ７は第２キーを受信し、以前受信した第２キーと照合することにより、所定の処理フローを経て認証結果が通知されたことを確認することができるようになる。

【００４４】バイオ認証サーバ５のバイオ認証処理部５３は、認証日時を認証処理結果ログＤＢ５９に登録する（ステップＳ１０３）。例えば、ＥＣサーバ７についての情報も認証処理結果ログＤＢ５９に格納しても良い。次に、後処理部５５は、登録バイオ・データの更新時期になったか否かを判断する（ステップＳ１０５）。例えば、所定周期ごとに登録バイオ・データを更新することになっている場合には、当該所定周期を経過したか否かを更新記録などを参照して判断する。

【００４５】もし、登録バイオ・データの更新時期ではないと判断された場合には、処理を終了する。一方、登録バイオ・データの更新時期であると判断された場合には、後処理部５５はユーザ端末３から受信した入力バイオ・データを会員バイオ情報ＤＢ５７に登録する（ステップＳ１０７）。これにて処理を終了する。なお、入力バイオ・データに対して処理を施した結果のデータを登録することもある。

【００４６】一方、ステップＳ９３において認証失敗と判断された場合には、バイオ認証処理部５３は認証処理回数は許容限度内（例えば３回）であるか判断する（ステップＳ１０９）。もし、認証処理回数が許容限度内であれば、ステップＳ８１に戻り、ユーザ端末３にバイオ・データの送信要求を送信する。一方、認証処理回数が許容限度を超えていれば、認証失敗をＥＣサーバ７及びユーザ端末３に送信する（ステップＳ１１１）。もし、キーを用いた処理系の場合には、このときに隠しパラメータとしてＥＣサーバ７に第２キーを送信する。

【００４７】ＥＣサーバ７は、バイオ認証サーバ５から認証失敗を受信すると（ステップＳ１１３）、認証要求を無効として取り扱う（ステップＳ１１５）。すなわち、発注受付を送信しないようにしたり、決済を実行したりせず、今回は受け付けられない旨の通知をユーザ端末３に行ったりする。また、ユーザ端末３は、認証失敗の情報を受信し（ステップＳ１１７）、処理を終了する。例えば、「今回認証できませんでした」といった表示を行う場合もある。

【００４８】バイオ認証サーバ５のバイオ認証処理部５３は、認証失敗を認証処理結果ログＤＢ５９に登録する（ステップＳ１１９）。

【００４９】以上のような処理を実施することにより、バイオ認証サーバ５における認証処理も実施することができるようになり、従ってユーザによる不正行為等を防止することができることができるようになる。

【００５０】以上本発明の一実施の形態を説明したが、本発明はこれに限定されるものではない。たとえば、ユーザ端末３にインストールされる認証処理プログラム３３は、図１に示した以外の機能を有するような場合もあ

る。例えば、電子マネーを取り扱うための機能や、その他の決済の処理を安全に実施するための機能等である。バイオ認証サーバ５及び認証処理プログラム３３の機能ブロックは、必ずしもプログラムのモジュールに対応しない。また、ＤＢの管理の仕方や分け方についても図１に示したものは一例である。

【００５１】さらに、図２乃至図５で説明した処理フローは一例であり、同様の処理を実施するためにステップの順番を入れ替えることも可能な部分もある。また、同時に実施することが可能なステップもある。

【００５２】なお、上で述べたような処理をコンピュータに実施させるプログラムを作成することも可能であって、当該プログラムは、例えばフレキシブル・ディスク、ＣＤ－ＲＯＭ、光磁気ディスク、半導体メモリ、ハードディスク等の記憶媒体又は記憶装置に格納される。なお、ネットワークを介して配布される場合もある。また、処理途中のデータについては、コンピュータのメモリに一時保管される。

【００５３】

【発明の効果】以上本発明により、センタ・サーバとユーザ端末とを含むシステムにおいてユーザ端末においてバイオメトリクス認証処理を実施するための技術を提供することができる。

【００５４】また、センタ・サーバにおいて必要な時に登録されたバイオメトリクス・データの更新を要求を行うことができるようにするための技術を提供することができる。

【００５５】さらに、センタ・サーバとユーザ端末とを含むシステムにおいてユーザ端末においてバイオメトリクス認証処理を安全に実施するための技術を提供することができる。

【図面の簡単な説明】

【図１】本発明の一実施の形態に係るシステム概要図である。

【図２】本発明の一実施の形態における処理フローを示す図である。

【図３】本発明の一実施の形態における処理フローを示す図である。

【図４】本発明の一実施の形態における処理フローを示す図である。

【図５】本発明の一実施の形態における処理フローを示す図である。

【符号の説明】

１　インターネット　　３　ユーザ端末　　５　バイオ認証サーバ

７　ＥＣサーバ　　３１　Ｗｅｂサーバ　　３３　認証処理プログラム

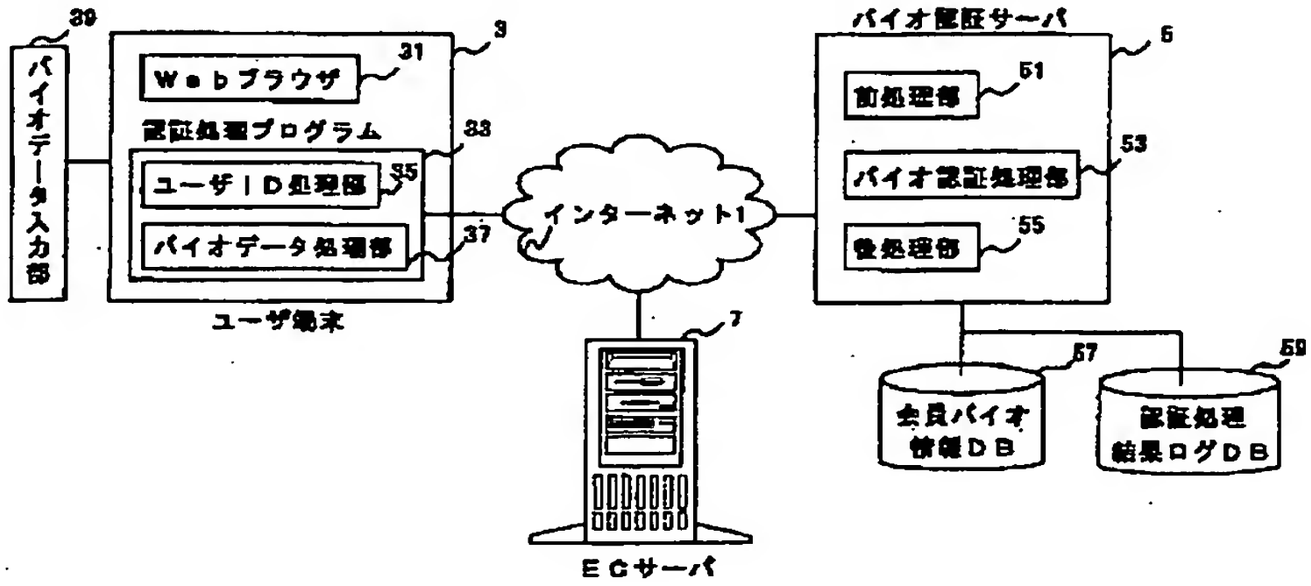
３５　ユーザＩＤ処理部　　３７　バイオデータ処理部

３９　バイオデータ入力部　　５１　前処理部

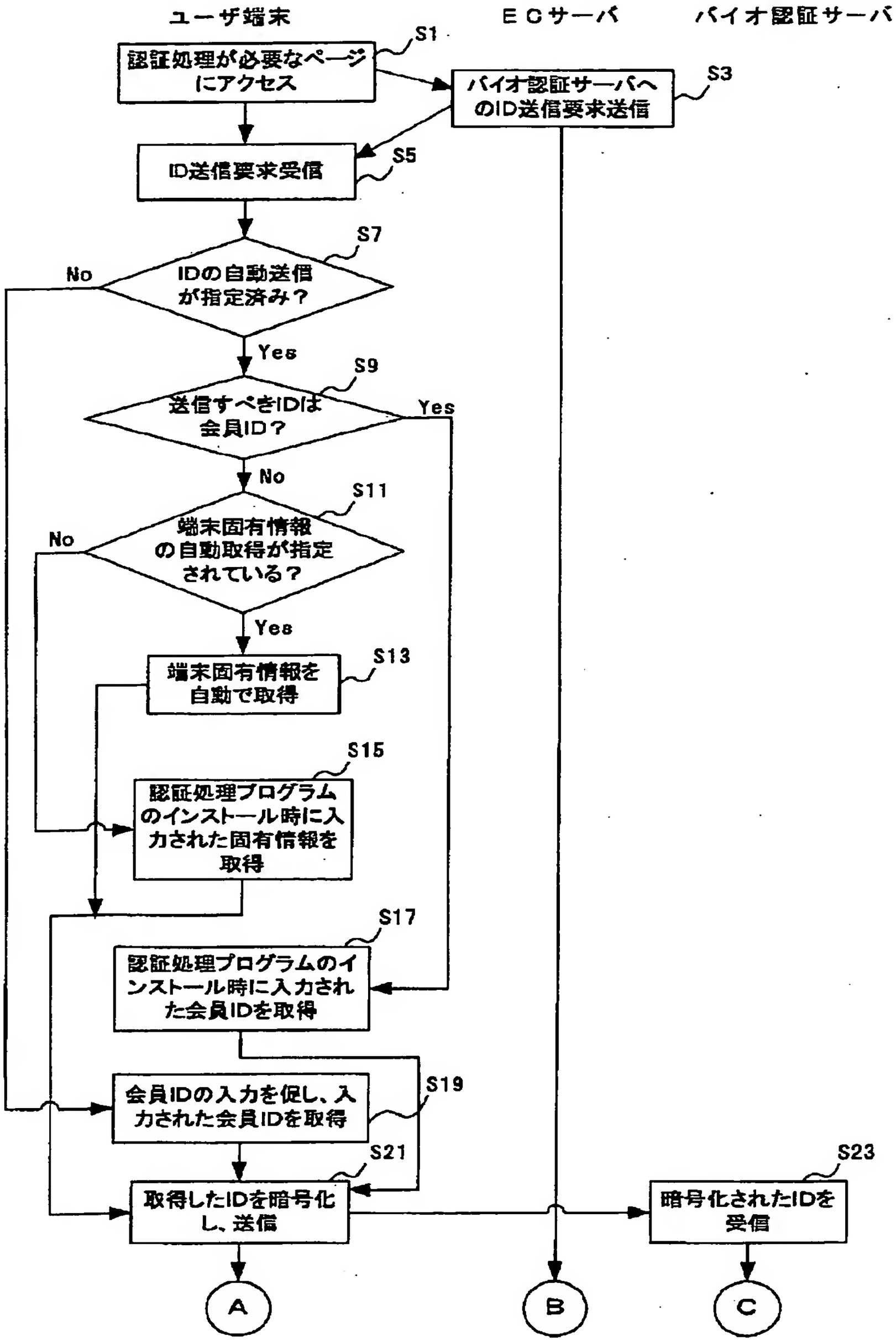
５３　バイオ認証処理部　　５５　後処理部

５７　会員バイオ情報ＤＢ　　５９　認証処理結果ログＤＢ

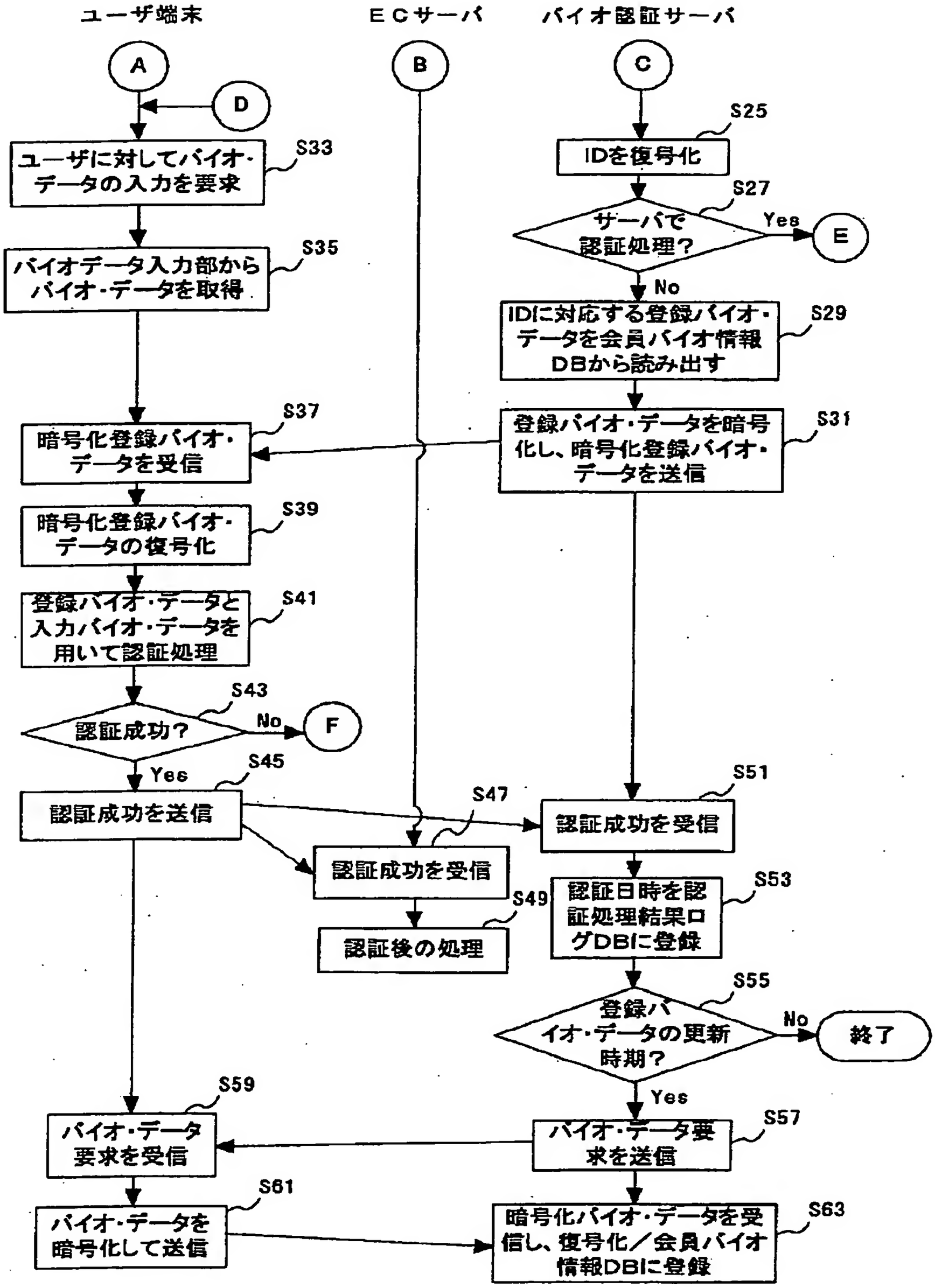
【図１】



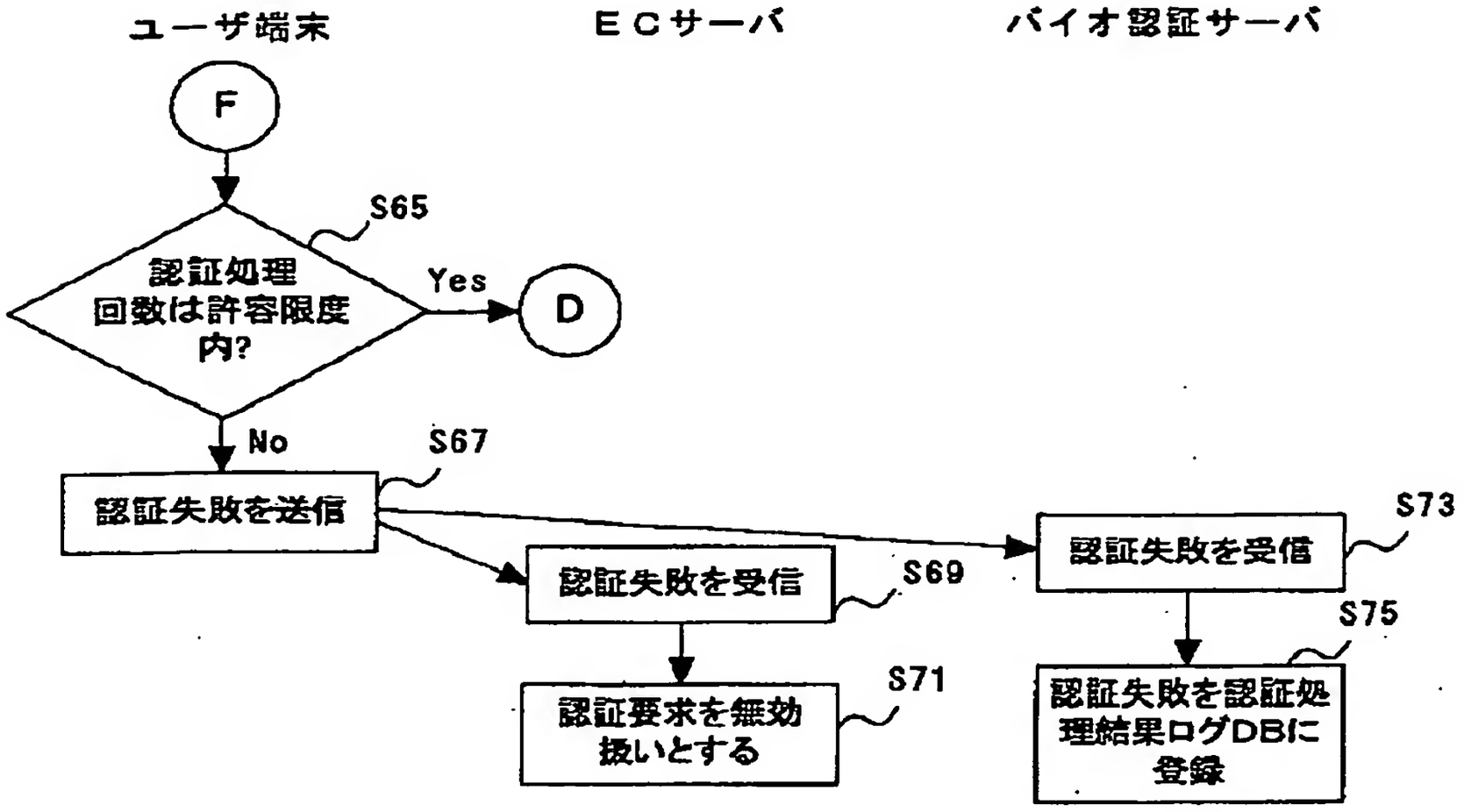
【図２】


ユーザ端末
ＥＣサーバ
バイオ認証サーバ
S1
認証処理が必要なページにアクセス
S3
バイオ認証サーバへのID送信要求送信
S5
ID送信要求受信
S7
IDの自動送信が指定済み？
No
Yes
S9
送信すべきIDは会員ID？
Yes
No
S11
端末固有情報の自動取得が指定されている？
No
Yes
S13
端末固有情報を自動で取得
S15
認証処理プログラムのインストール時に入力された固有情報を取得
S17
認証処理プログラムのインストール時に入力された会員IDを取得
S19
会員IDの入力を促し、入力された会員IDを取得
S21
取得したIDを暗号化し、送信
S23
暗号化されたIDを受信
A
B
C

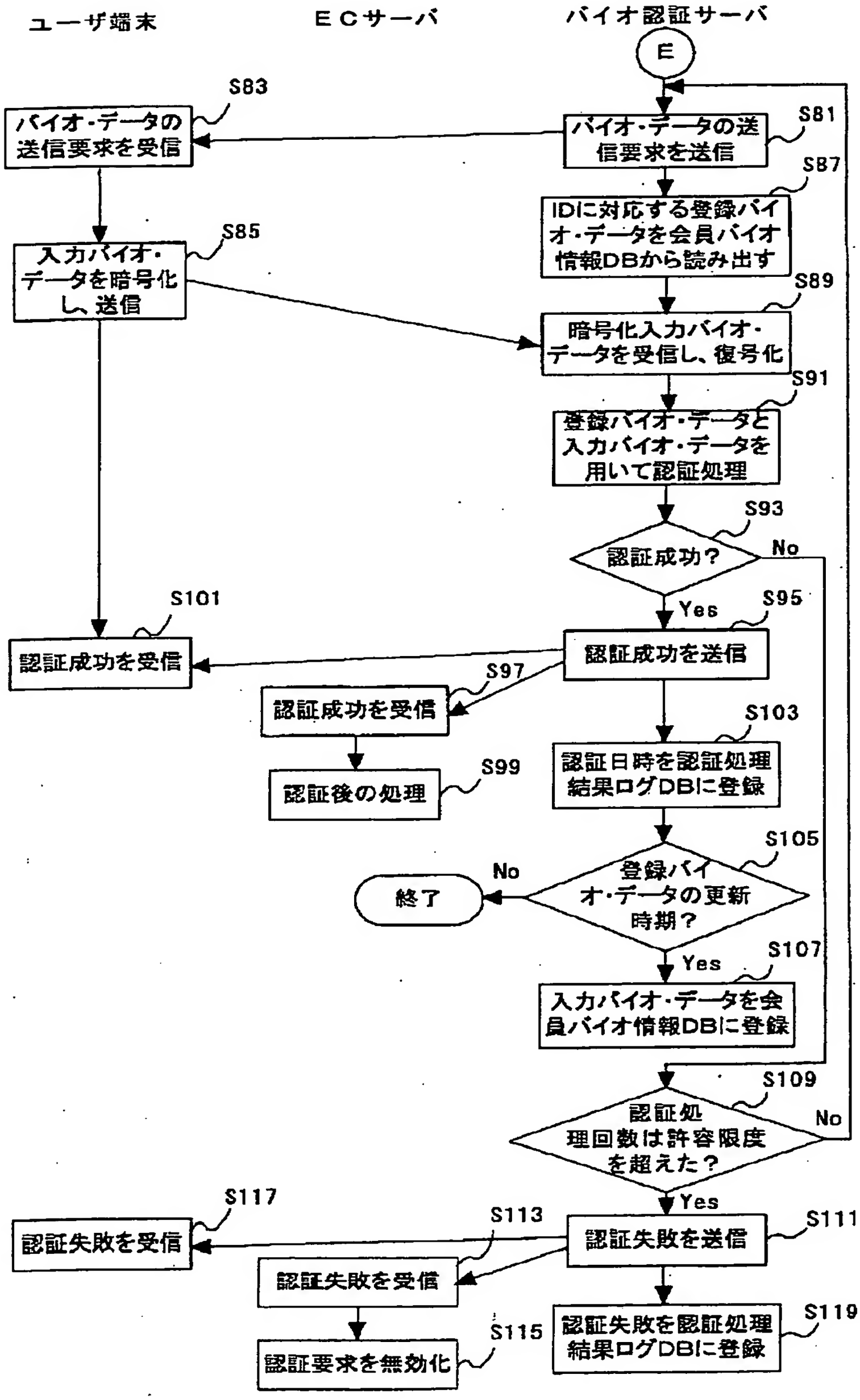
【図３】


ユーザ端末
ＥＣサーバ
バイオ認証サーバ
A
D
B
C
S25
IDを復号化
S27
サーバで認証処理？
Yes
E
No
IDに対応する登録バイオ・データを会員バイオ情報DBから読み出す
S29
登録バイオ・データを暗号化し、暗号化登録バイオ・データを送信
S31
S33
ユーザに対してバイオ・データの入力を要求
S35
バイオデータ入力部からバイオ・データを取得
S37
暗号化登録バイオ・データを受信
S39
暗号化登録バイオ・データの復号化
S41
登録バイオ・データと入力バイオ・データを用いて認証処理
S43
認証成功？
No
F
Yes
S45
認証成功を送信
S47
認証成功を受信
S49
認証後の処理
S51
認証成功を受信
S53
認証日時を認証処理結果ログDBに登録
S55
登録バイオ・データの更新時期？
No
終了
Yes
S57
バイオ・データ要求を送信
S59
バイオ・データ要求を受信
S61
バイオ・データを暗号化して送信
S63
暗号化バイオ・データを受信し、復号化／会員バイオ情報DBに登録

【図４】


ユーザ端末
ＥＣサーバ
バイオ認証サーバ
F
S65
認証処理回数は許容限度内?
Yes
D
No
S67
認証失敗を送信
認証失敗を受信
S69
認証失敗を受信
S73
S75
認証要求を無効扱いとする
S71
認証失敗を認証処理結果ログDBに登録

【図５】


ユーザ端末
ＥＣサーバ
バイオ認証サーバ
E
S81
バイオ・データの送信要求を送信
S83
バイオ・データの送信要求を受信
S85
入力バイオ・データを暗号化し、送信
S87
IDに対応する登録バイオ・データを会員バイオ情報DBから読み出す
S89
暗号化入力バイオ・データを受信し、復号化
S91
登録バイオ・データと入力バイオ・データを用いて認証処理
S93
認証成功？
No
Yes
S95
認証成功を送信
S97
認証成功を受信
S99
認証後の処理
S101
認証成功を受信
S103
認証日時を認証処理結果ログDBに登録
S105
登録バイオ・データの更新時期？
No
終了
Yes
S107
入力バイオ・データを会員バイオ情報DBに登録
S109
認証処理回数は許容限度を超えた？
No
Yes
S111
認証失敗を送信
S113
認証失敗を受信
S115
認証要求を無効化
S117
認証失敗を受信
S119
認証失敗を認証処理結果ログDBに登録